What is claimed is:

Claims

1. A method comprising the steps of:

generating a random number, an expected response, and a derived cipher key;

forwarding the random number and a random seed to a base station;

receiving, from the base station, a response to the random number and the random seed;

comparing the response and the expected response;

when the response matches the expected response, forwarding the derived cipher key to the base station.

2. The method of claim 1, further comprising the step of, when the response does not match the expected response, discarding the derived cipher key without forwarding the derived cipher key to the base station.

3. The method of claim 2, further comprising the step of sending a failed authentication message to the base station.

4. The method of claim 1, wherein the expected response is generated at least indirectly from the random number and the random seed.

5. The method of claim 1, wherein the derived cipher key is generated at least indirectly from the random number and the random seed.

6. The method of claim 1, wherein the derived cipher key is stored at a visited location register.

7. The method of claim 1, wherein the derived cipher key is encrypted by an intrakey and stored at a visited location register.

8. The method of claim 1, wherein the derived cipher key is stored at a home location register.

9. The method of claim 1, wherein the derived cipher key is encrypted by an intrakey and stored at a home location register.

10. The method of claim 1, wherein the steps are performed by a zone controller.

11. The method of claim 1, wherein the steps are performed by a visited location register.

12. The method of claim 1, wherein the response is generated by a mobile station.

13. The method of claim 1, wherein the base station is located in a zone and wherein the derived cipher key is encrypted by an intrakey when transferred within the zone before being forwarded to the base station.

14. The method of claim 1, wherein any of a base site and a TETRA site controller takes the place of the base station.

15. The method of claim 1, further comprising the steps of:

receiving, from the base station, a second random number generated by a mobile station;

generating a second derived cipher key and a second response to the second random number and forwarding the second response to the base station;

combining the derived cipher key and the second derived cipher key, yielding a third derived cipher key;

when a positive authentication message is received from the base station, forwarding the third derived cipher key to the base station.

16. A method performed by any of a base station and comprising the steps of:

receiving an authentication request from a mobile station;

determining whether to forward the request to an authentication agent;

when it is determined to forward the request, forwarding the request to the authentication agent;

receiving a random number and a random seed from the authentication agent;

forwarding the random number and the random seed to the mobile station;

receiving a response to the random number and the random seed from the mobile station and forwarding the response to the authentication agent;

when the authentication agent authenticates the mobile station, receiving a derived cipher key from the authentication agent;

encrypting messages to the mobile station and decrypting messages from the mobile station with the derived cipher key.

17. The method of claim 16, further comprising the step of, when the authentication agent sends a negative authentication to the base station, forwarding the negative authentication to the mobile station.

18. The method of claim 16, wherein the authentication agent is a zone controller.

19. The method of claim 16, wherein the authentication agent is a visited location register.

20. The method of claim 16, wherein the base station is located in a zone and wherein the derived cipher key is encrypted by an intrakey when transferred within the zone before being forwarded to the base station.

21. The method of claim 16, wherein any of a base site and a TETRA site controller takes the place of the base station.

22. The method of claim 16:

receiving a second random number from a mobile station;

forwarding the second random number to the authentication agent;

receiving a second response to the second random number from the authentication agent;

forwarding the second response to the mobile station;

when the mobile station authenticates the infrastructure, forwarding an authenticated message to the authentication agent;

receiving a second derived cipher key from the authentication agent;

encrypting messages to the mobile station and decrypting messages from the mobile station with the second derived cipher key.

23. A method comprising the steps of:

receiving, from a base station, a random number generated by a mobile station;

using a random seed, generating a derived cipher key and a response to the random number and forwarding the random seed and the response to the base station;

when a positive authentication message is received from the base station, forwarding the derived cipher key to the base station.

24. The method of claim 23, further comprising the step of, when a negative authentication message is received from the base station, discarding the derived cipher key without forwarding the derived cipher key to the base station.

25. The method of claim 23, wherein the response is generated at least indirectly from the random number and the random seed.

26. The method of claim 23, wherein the derived cipher key is generated at least indirectly from the random number and the random seed.

27. The method of claim 23, wherein the derived cipher key is stored at a visited location register.

28. The method of claim 23, wherein the derived cipher key is encrypted by an intrakey and stored at a visited location register.

29. The method of claim 23, wherein the derived cipher key is stored at a home location register.

30. The method of claim 23, wherein the derived cipher key is encrypted by an intrakey and stored at a home location register.

31. The method of claim 23, wherein the steps are performed by a zone controller.

32. The method of claim 23, wherein the steps are performed by a visited location register.

33. The method of claim 23, wherein the base station is located in a zone and wherein the derived cipher key is encrypted by an intrakey when transferred within the zone before being forwarded to the base station.

34. The method of claim 23, wherein any of a base site and a TETRA site controller takes the place of the base station.

35. The method of claim 23, wherein the method is of a mutual authentication process.

36. A method performed by a base station and comprising the steps of:

receiving a random number from a mobile station;

forwarding the random number to an authentication agent;

receiving a response to the random number and a random seed from the authentication agent;

forwarding the response and the random seed to the mobile station;

when the mobile station authenticates the infrastructure, forwarding an authenticated message to the authentication agent;

receiving a derived cipher key from the authentication agent;

encrypting messages to the mobile station and decrypting messages from the mobile station with a derived cipher key.

37. The method of claim 36, further comprising the step of, when the mobile station sends a negative authentication to the base station, forwarding the negative authentication to the authentication agent, which discards the derived cipher key.

38. The method of claim 36, wherein the authentication agent is a zone controller.

39. The method of claim 36, wherein the authentication agent is a visited location register.

40. The method of claim 36, wherein the base station is located in a zone and wherein the derived cipher key is encrypted by an intrakey when transferred within the zone before being forwarded to the base station.

41. The method of claim 36, wherein any of a base site and a TETRA site controller takes the place of the base station.

42. A system comprising:

a first system device in a first zone of the system, the first system device comprised of memory for storing:

first zone session authentication information,

a first key for encrypting at least one of key material and a part of the first zone session authentication information for transport in real-time to another system device in the first zone, and

a second key for encrypting at least a segment of the first zone session authentication information for transport to a system device in a zone other than the first zone;

a second system device comprised of memory for storing the first zone session authentication information at least partially in an encrypted form.

43. The system of claim 42, wherein the first system device is a zone controller.

44. The system of claim 42, wherein the first system device is a visited location register.

45. The system of claim 42, wherein the first system device is a home location register.

46. The system of claim 42, wherein the second system device is a zone manager.

47. The system of claim 42, wherein the another system device in the first zone is any of a base station, a base site, and a TETRA site controller.

48. The system of claim 42, wherein the first zone session authentication information is stored at least partially encrypted in the first system device.

49. The system of claim 42, wherein the first key is an intrakey associated with the first zone.

50. The system of claim 42, wherein the first key is an interkey.

51. The system of claim 42, wherein the second key is an interkey.

52. The system of claim 42, further comprising:

a third system device in a second zone of the system, the third system device comprised of memory for storing:

second zone session authentication information,

a third key for encrypting at least one of key material and a part of the second zone session authentication information for transport in real-time to another system device in the second zone, and

the second key for encrypting at least a segment of the second zone session authentication information for transport to a system device in a zone other than the second zone.

53. The system of claim 52, wherein the third system device is a zone controller.

54. The system of claim 52, wherein the third system device is a visited location register.

55. The system of claim 52, wherein the third system device is a home location register.

56. The system of claim 52, wherein the another system device in the second zone is any of a base station, a base site, and a TETRA site controller.

57. The system of claim 52, wherein the second zone session authentication information is stored at least partially encrypted in the third system device.

58. The system of claim 52, wherein the third key is an intrakey associated with the second zone.

59. The system of claim 52, further comprising a fourth system device comprised of memory for storing the second zone session authentication information at least partially in encrypted form.

60. The system of claim 59, wherein the fourth system device is a zone manager.

61. The system of claim 59, further comprising a fifth system device comprised of memory for storing system session authentication information comprising at least the first zone session authentication information and the second zone session authentication information at least partially in encrypted form.

62. The system of claim 61, wherein the fifth system device is a user configuration server.

63. The system of claim 61, further comprising:

a sixth system device comprised of:

memory for storing authentication key information;

a processor, operably coupled to the memory, the processor arranged and constructed to generate the system session authentication information from the authentication key information, and encrypt the system session authentication information for transport to at least the fifth system device in non-real-time.

64. The system of claim 63, wherein the sixth system device is an authentication center.

65. The system of claim 63, wherein the sixth system device is a key management facility.

66. The system of claim 63, wherein the authentication key information is hardware encrypted before storage in the sixth device.

67. The system of claim 63, wherein the session authentication information comprises at least two keys utilized in an encryption authentication process.

68. A method comprising the steps of:

generating session authentication information for each of a plurality of authentication keys for use in a communication system;

encrypting the session authentication information;

forwarding the encrypted session authentication information to a storage device for access in a non-real-time manner.

69. The method of claim 68, further comprising the step of storing the plurality of keys as encrypted data.

70. The method of claim 69, wherein at least one of the plurality of keys is encrypted by a hardware-based encryption device.

71. The method of claim 68, wherein the session authentication information is encrypted by a software-based encryption device.

72. The method of claim 68, wherein the session authentication information is encrypted with an interkey.

73. The method of claim 68, wherein the storage device is a user configuration server.

74. The method of claim 68, further comprising the step of forwarding, by the storage device, at least a part of the encrypted session authentication information to a first system device at a zone in the communication system in a non-real-time manner.

75. The method of claim 74, wherein the part of the encrypted session authentication information includes session authentication information for at least one mobile station registered at the zone.

76. The method of claim 74, further comprising the step of forwarding, by the first system device, at least some of the at least a part of the encrypted session authentication information to a home location register at the zone in a non-real-time manner.

77. The method of claim 76, further comprising the step of decrypting, by the second system device, the at least some of the at least a part of the encrypted session authentication information, yielding decrypted session authentication information.

78. The method of claim 77, further comprising the step of encrypting, by the second system device, at least a part of the decrypted session authentication information, yielding re-encrypted session authentication information.

79. The method of claim 78 wherein the step of encrypting at least the part of the decrypted session authentication information comprises the step of encrypting the at least the part of the decrypted session authentication information using an intrakey.

80. The method of claim 78, wherein the step of encrypting at least the part of the decrypted session authentication information comprises the step of encrypting the at least the part of the decrypted session authentication information using an interkey.

81. The method of claim 78, further comprising the step of forwarding, by the second system device, the re-encrypted session authentication information to a third system device in a real-time manner.

82. The system of claim 78, wherein the session authentication information comprises at least two keys utilized in an encryption authentication process.

83. A system comprising:

a key management facility, arranged and constructed to store an authentication key for each mobile station residing in the system;

a user configuration server, operably coupled to the key management facility, arranged and constructed to store and distribute session authentication information for each mobile station residing in the system;

a zone manager, operably coupled to the user configuration server, arranged and constructed to store relevant session authentication information for a zone managed by the zone manager and to distribute the relevant session authentication information to a home location register within a zone controller for the zone;

wherein the key management facility, user configuration server, and the zone manager are arranged and constructed to provide the session authentication information to each other or to a zone in the even of a fault in the system;

wherein the home location register is arranged and constructed to continue to provide authentication and support secure communications in the event of a fault at any of the key management facility, user configuration server, and the zone manager.

84. The system of claim 83, further comprising a visited location register, arranged and constructed to continue to provide authentication and support secure communications in the event of a fault at any of the key management facility, user configuration server, and the zone manager, and wherein at least part of the relevant session authentication information is distributed to the visited location register.

85. The system of claim 83, wherein the zone controller generates a derived cipher key from the session authentication information during an authentication process.

86. The system of claim 83, wherein the session authentication information comprises at least two keys utilized in an encryption authentication process.

87. A system comprising:

a plurality of first-level system devices, arranged and constructed to encrypt, store, and forward at least some session authentication information in a non-real-time manner;

a plurality of second-level system devices, arranged and constructed to receive at least a part of the session authentication information from at least one of the plurality of first-level system devices in a real-time manner.

88. The system of claim 87, wherein at least one of the plurality of first-level system devices generates the session authentication information.

89. The system of claim 87, wherein the plurality of second-level system devices authenticates one or more mobile stations in a real-time manner based on the session authentication information.

90. The system of claim 87, wherein the plurality of first-level system devices comprises a key management facility, a user configuration server, and at least one zone manager.

91. The system of claim 87, wherein the plurality of second-level system devices comprises at least one zone controller and at least one base station.

92. The system of claim 87, wherein at least one of the plurality of first-level system devices is arranged and constructed to encrypt the session authentication information using an interkey.

93. The system of claim 87, wherein the plurality of second-level system devices is arranged and constructed to encrypt at least a segment of the session authentication information using an interkey when the encrypted session authentication information is forwarded to a system device in a zone other than the zone in which the forwarding device is located.

94. The system of claim 87, wherein the plurality of second-level system devices is arranged and constructed to encrypt at least a segment of the session authentication information using one of an intrakey and an interkey when the encrypted session authentication information is forwarded to a system device in a zone in which the forwarding device is located.

95. A method comprising the steps of:

receiving, from a mobile station, a request to communicate in a communication system;

determining whether the request is encrypted;

when the request is not encrypted, sending a request to authenticate the mobile station to an infrastructure device in the communication system;

when the request is encrypted, determining whether the mobile station is powering up;

when the mobile station is powering up and the request is encrypted, sending a request to authenticate the mobile station to the infrastructure device in the communication system;

when the mobile station is not powering up and the request is encrypted, determining whether the request is encrypted using a valid key;

when the mobile station is not powering up and the request is encrypted using a valid key, permitting the mobile station access to the system without requesting authentication.

96. The method of claim 95, further comprising the steps of:

storing authentication requests during a time period when the infrastructure device is not available;

when the infrastructure device becomes available, forwarding the stored authentication requests to the infrastructure device.

97. A method comprising the steps of:

receiving, from a mobile station, a request to communicate in a communication system;

determining whether the mobile station is powering up;

when the mobile station is powering up, sending a request to authenticate the mobile station to an infrastructure device in the communication system;

when the mobile station is not powering up, determining whether the request is encrypted;

when the request is not encrypted, sending a request to authenticate the mobile station to an infrastructure device in the communication system;

when the mobile station is not powering up and the request is encrypted, determining whether the request is encrypted using a valid key;

when the mobile station is not powering up and the request is encrypted using a valid key, permitting the mobile station access to the system without requesting authentication.

98. The method of claim 97, further comprising the steps of:

storing authentication requests during a time period when the infrastructure device is not available;

when the infrastructure device becomes available, forwarding the stored authentication requests to the infrastructure device.